

Claims

1. A method for providing secure access to a packet data network, said
method comprising:
- 5 a) receiving a message from a terminal device (40, 60), connected to said
packet data network;
- b) deriving a first source information from said message;
- c) deriving a second source information;
- d) comparing said first and second source information; and
- e) initiating a protection processing based on the result of said comparing
10 step.
2. A method according to claim 1, wherein said first source information is a
source address information derived from a header portion of said message.
- 15 3. A method according to claim 1 or 2, wherein said second source information
is a source address information derived from a packet data unit used for
conveying said message, or from a security association set up between
said terminal device (40, 60) and said packet data network.
- 20 4. A method according to any one of the preceding claims, wherein said pro-
tection processing comprises a processing for dropping said message if
said comparing step leads to the result that said first source information and
said second source information do not indicate the same location.
- 25 5. A method according to any one of the preceding claims, wherein said pro-
tection processing comprises a processing for dropping said message if
said comparing step leads to the result that said first source information and
said second source information do not match.
6. A method according to any one of the preceding claims, wherein said first
source information is an IP address.
7. A method according to claim 6, wherein said message is a SIP message.
- 30 8. A method according to any one of the preceding claims, wherein said sec-
ond source information is at least a part of an IP source address of an IP
datagram.

9. A method according to claim 8, wherein said datagram is transmitted using an IP security protocol.
10. A method according to claim 3, wherein said second source information is an IP address bound to an integrity key of said security association.
- 5 11. A method according to claim 10, wherein said IP address is stored in a database of a proxy server (30) provided for routing said message to said packet data network.
12. A method according to claim 10 or 11, wherein said message is conveyed using a SIP-level protection function.
- 10 13. A network element for providing secure access to a packet data network, said network element (30) comprising:
 - a) receiving means (31) for receiving a message from a terminal device (40, 60) connected to said network element (30);
 - b) deriving means (31) for deriving a first source information from said message, and for deriving a second source information;
 - c) comparing means (33) for comparing said first and second source information; and
 - d) protecting means (32) for initiating a protection processing based on the comparing result of said comparing means.
- 20 14. A network element according to claim 13, wherein said deriving means (31) is arranged for deriving said second source information from a packet data unit used for conveying said message or from a security association set up between said terminal device (40, 60) and said network element (30).
- 25 15. A network element according to claim 13 or 14, wherein said deriving means (31) is arranged for deriving said first source information from a header portion of said message.
- 30 16. A network element according to any one of claims 13 to 15, wherein said protecting means (32) are arranged to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not indicate the same location.

- 17. A network element according to any one of claims 13 to 15, wherein said protecting means (32) are arranged to initiate a processing for dropping said message if said comparing result indicates that said first source information and said second source information do not match.
- 5 18. A network element according to any one of claims 13 to 17, wherein said deriving means are arranged for reading said second source information from a database (34) provided at said network element.
- 10 19. A network element according to any one of claims 13 to 18, wherein said deriving means (31) are arranged for deriving said second source information by extracting an IP source address from an IP datagram.
- 20. A network element according to any one of claims 13 to 19, wherein said network element is a proxy server (30).
- 15 21. A network element according to claim 20, wherein said proxy server is a P-CSCF (30) of an IP Mobility Subsystem.